

FIG. 1

## **REGISTRATION PHASE**

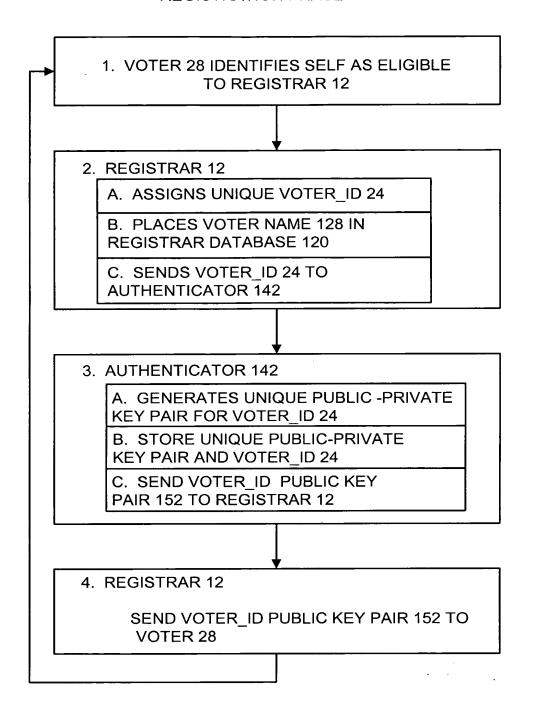


FIG. 1A 2 OF 16

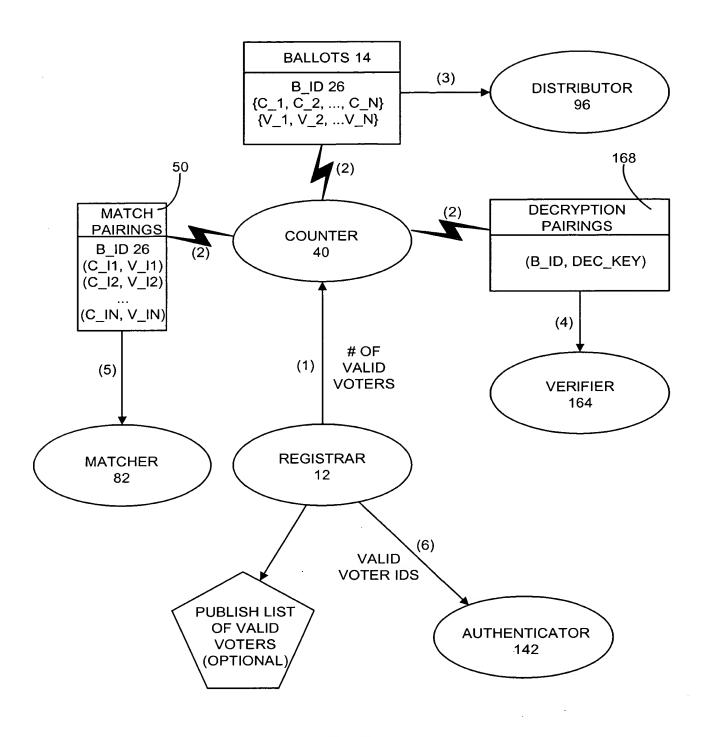


FIG. 2 3 OF 16

## PRE-VOTING PHASE

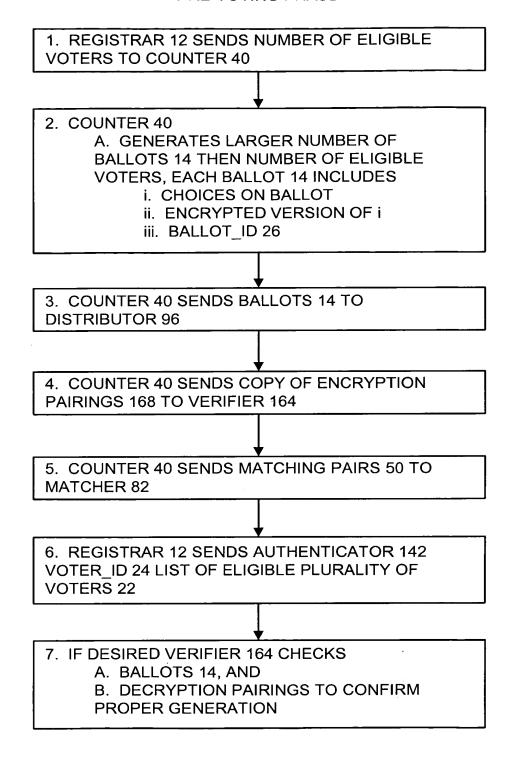


FIG. 2A 4 OF 16

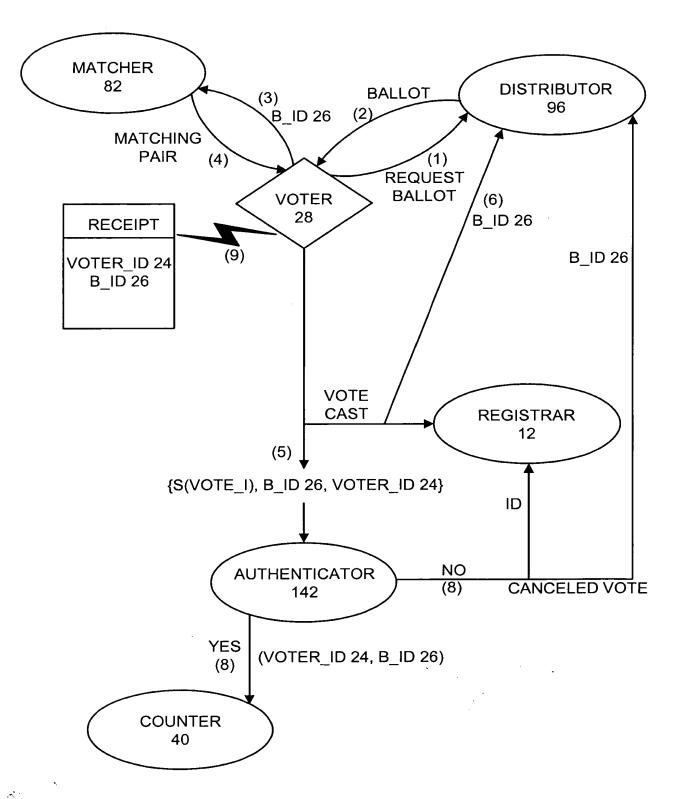


FIG. 3 5 OF 16

## **VOTING PHASE**

1. VOTER 28 ASKS DISTRIBUTOR 96 FOR BALLOT 14 2. DISTRIBUTOR 96 A. RANDOMLY SELECTS A BALLOT 14 B. SENDS SELECTED BALLOT 14 TO VOTER 28 3. VOTER 28 REQUESTS MATCHER 82 FOR MATCHING PAIR 50 FOR BALLOT 14 (e.g., THROUGH HIS WEB BROWSER) 4. MATCHER 82 SENDS VOTER 28 APPROPRIATE MATCHING PAIR 50 5. VOTER 28 A. SIGNS ENCRYPTED VERSION OF DESIRED VOTE B. SENDS AUTHENTICATOR 142 DESIRED VOTE, SIGNATURE, BALLOT ID 26 AND VOTER ID 24 6. VOTER 28 (e.g., THROUGH HIS WEB BROWSER) INFORMS DISTRIBUTOR 96 THAT BALLOT 14 WITH GIVEN BALLOT ID 26 HAS BEEN CAST 7. VOTER 28 (e.g., THROUGH HIS WEB BROWSER) INFORMS REGISTRAR 12 THAT VOTER 28 HAS CAST VOTE 8. AUTHENTICATOR 142 A. CHECKS SIGNATURE TO AUTHENTICATE VOTE B. IF AUTHENTIC, PASSES ENCRYPTED VOTE TO COUNTER 40 WITH BALLOT ID 26 9. VOTER 28 OBTAINS RECEIPT FROM AUTHENTICATOR 142

> FIG. 3A 6 OF 16

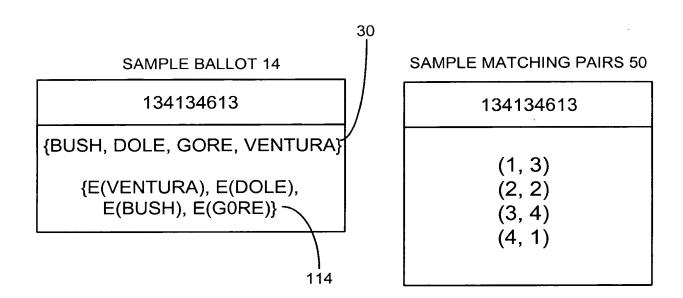


FIG. 4 7 OF 12

## ANNOUNCEMENT PHASE

- 1. COUNTER 40
  - A. DECRYPTS RECEIVED VOTES
  - **B. TALLIES VOTES**
- 2. AUTHENTICATOR 142 PUBLISHES LIST #1 OF
  - i. ENCRYPTED BALLOTS, AND
  - ii. BALLOT IDS
- 3. COUNTER 40
  - A. PUBLISHES LIST #2 CONTAINING ITS VERSION OF
    - i. ENCRYPTED BALLOTS, AND
    - ii. BALLOT IDS
  - B. LIST #1 AND LIST #2 SHOULD BE IDENTICAL
- 4. AUTHENTICATOR 142 PUBLISHES LIST #3 OF ALL VOTER\_IDS 24 THAT CAST BALLOTS 14
- 5. REGISTRAR 12 LOOKS AT LIST #1 TO VERIFY THAT ONLY ELIGIBLE VOTERS 38 VOTED
- 6. VERIFIER 164 CONFIRMS THAT LIST #1 AND LIST #2 ARE IDENTICAL
- 7. VERIFIER 164 USES LIST #1 AND THE DECRYPTION PAIRS 168 TO CONFIRM RESULTS OF COUNTER 40
- 8. VOTERS 22 CAN LOOK AT LIST#1 AND LIST #2 TO SEE THEIR VOTES ON THESE LISTS
- 9. DISTRIBUTOR 96
  - A. LOOKS AT LIST #1 AND LIST #2 TO ENSURE ONLY ELIGIBLE BALLOTS
  - B. REMOVE INELIGIBLE BALLOTS
  - C. OPTIONALLY, RELEASE LIST OF BALLOT IDS 26
- 10. COUNTER 40 ANNOUNCES ELECTION RESULTS WHICH MAY BE OPTIONALLY VERIFIED BY VERIFIER 164

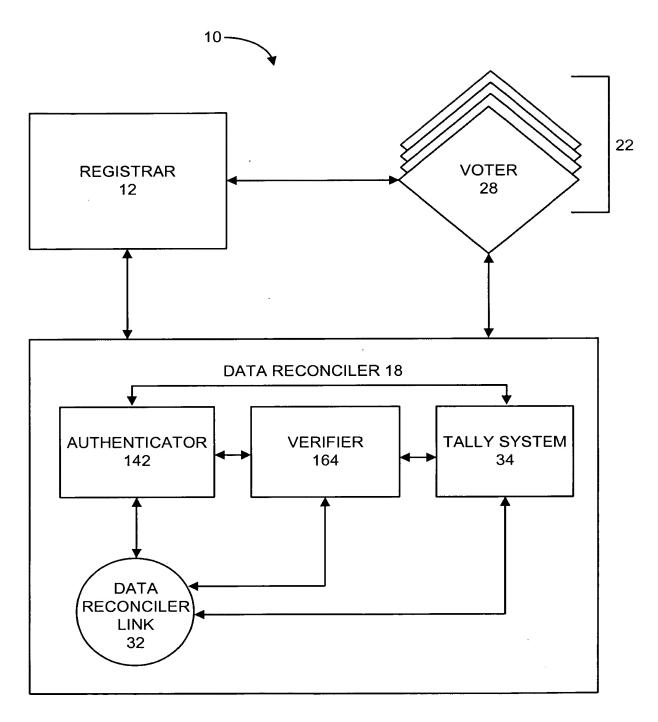


FIG. 5 9 of 16

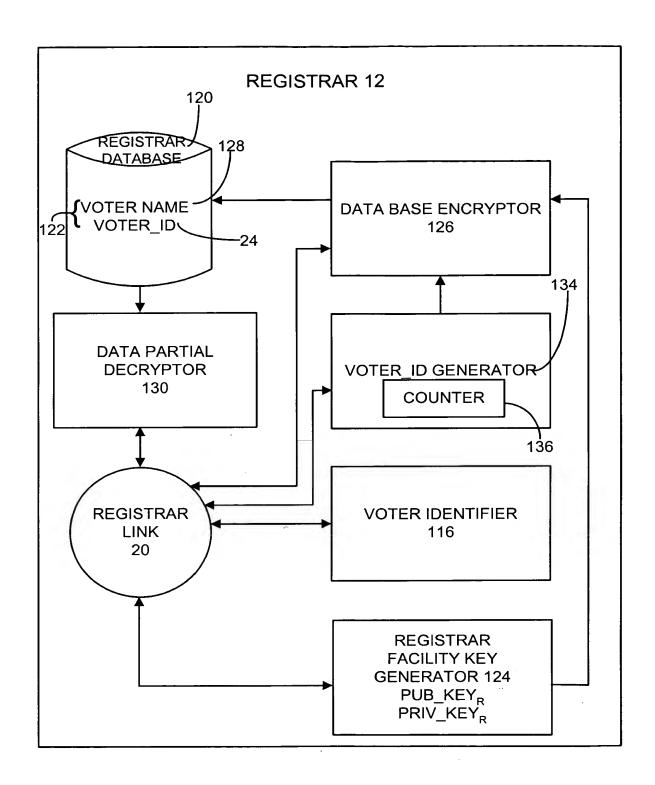


FIG. 6

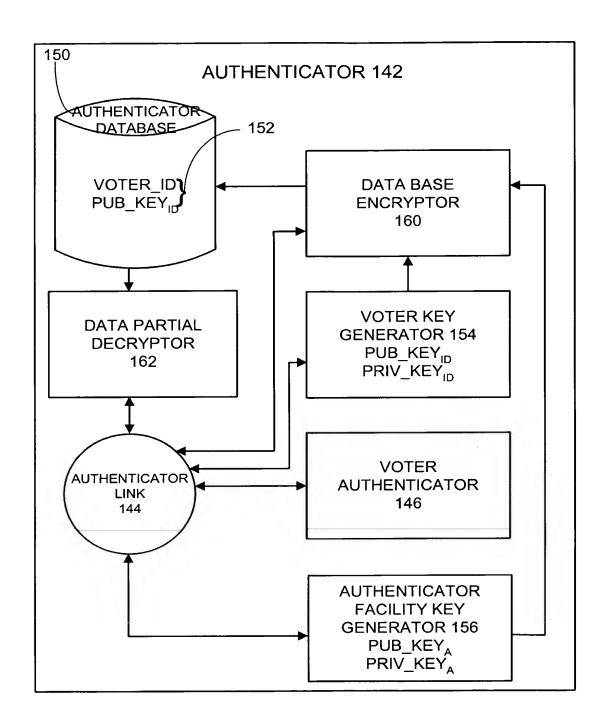


FIG. 7

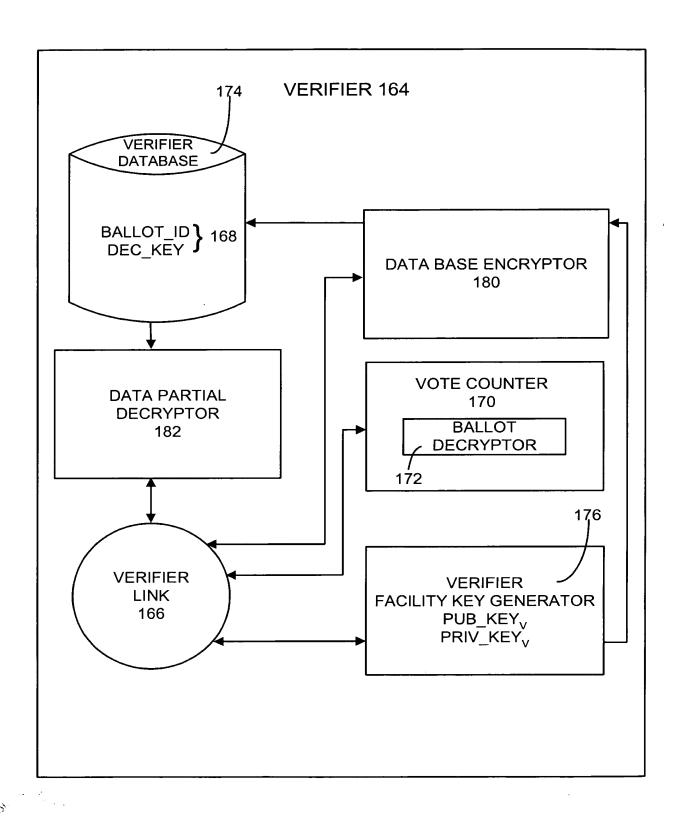


FIG. 8 12 OF 16

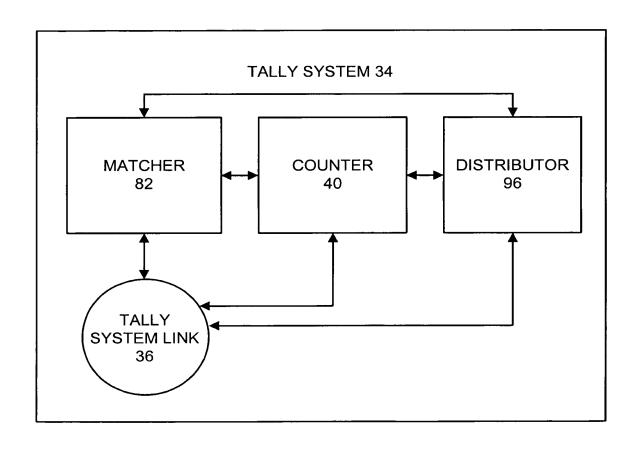


FIG. 9

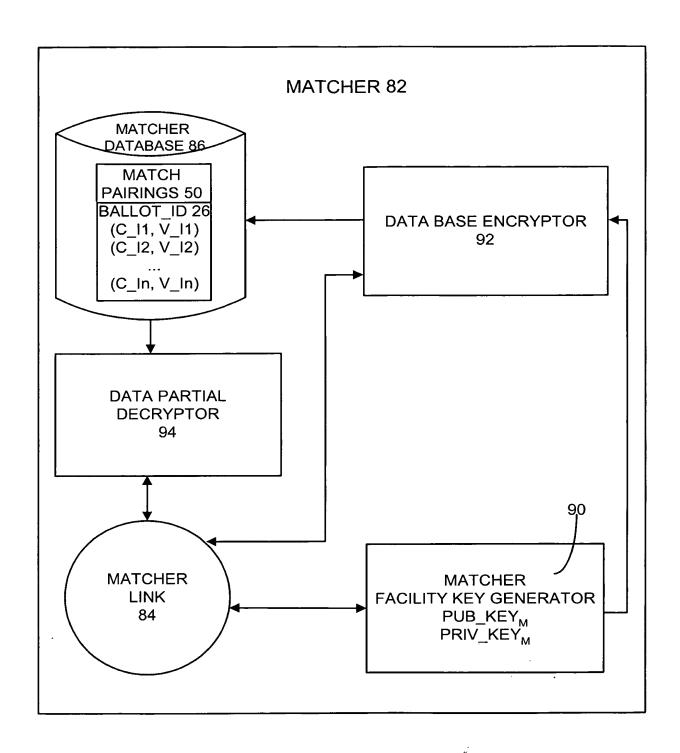


FIG. 10 14 OF 16

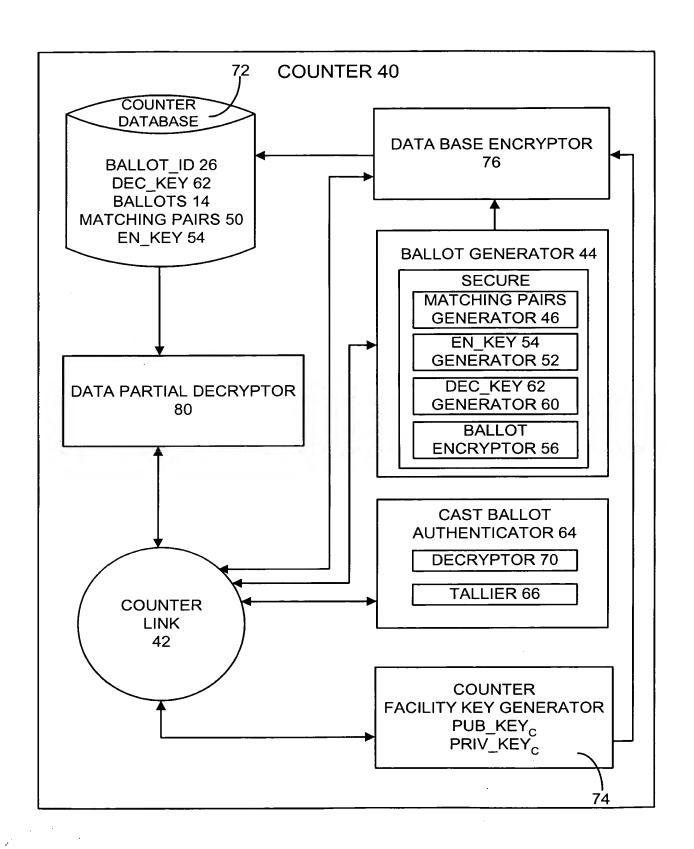


FIG. 11 15 OF 16

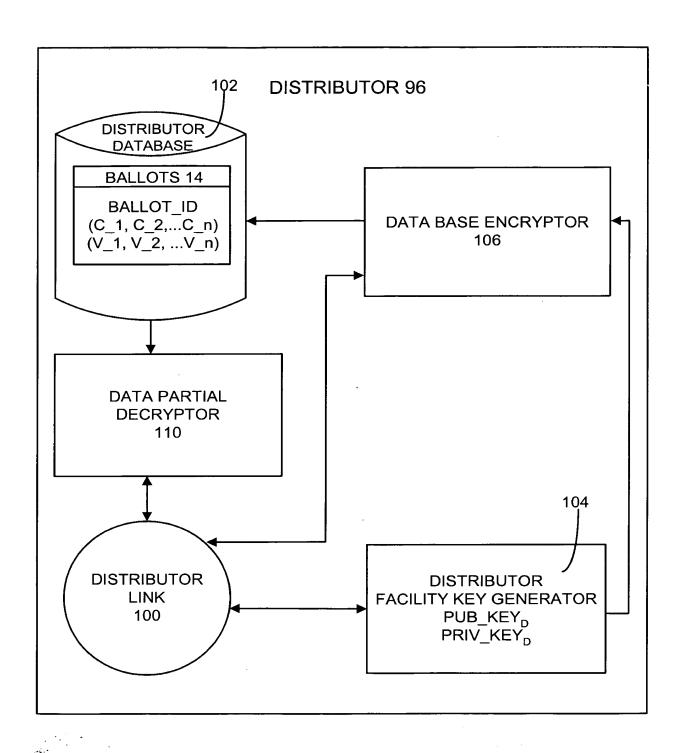


FIG. 12